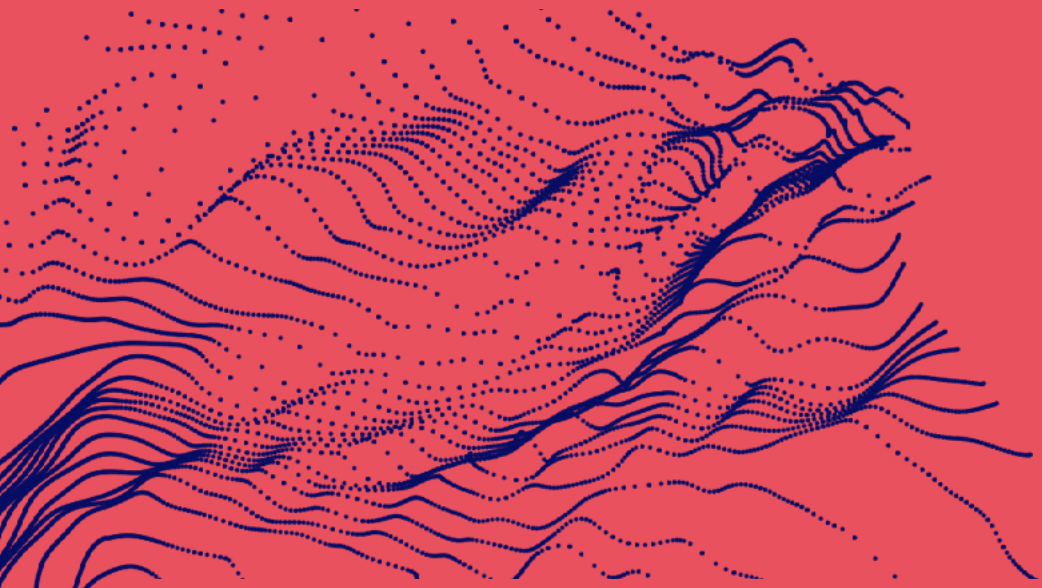
WHITE PAPER



NETWORK RESILIENCE

THE ROLE OF SATELLITE IN RESILIENT CRITICAL COMMUNICATIONS

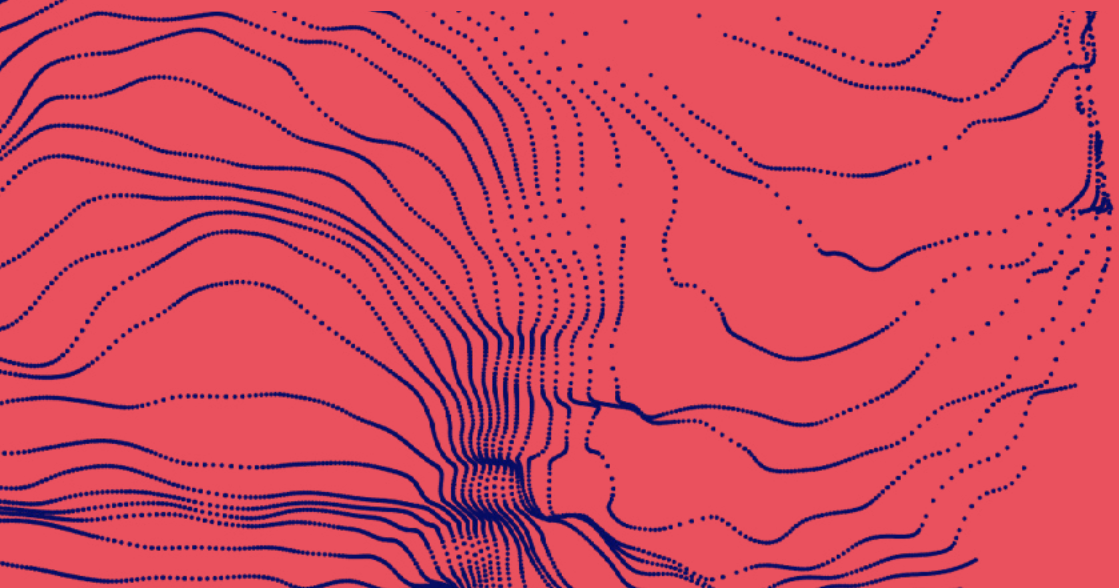


TABLE OF CONTENTS

EXECUTIVE SUMMARY

Modern governments, emergency responders, utilities, and critical enterprises rely on networks that must remain operational under adverse conditions. As physical hazards, cyber threats, and geopolitical shocks can be frequent and severe, **network resilience** is shifting firmly towards **strategic priority and regulatory requirement**. Single domain connectivity (for example, terrestrial only backbones) can fail in correlated ways — from storm damage and power loss to cable cuts — causing a cascade of service impacts. Subsea cable incidents which have slowed traffic between regions, even after rerouting, illustrate this systemic exposure.

Resilience means preventing, withstanding, recovering from, and **adapting** to disruption while maintaining acceptable performance. That requires **diversity of access paths, intelligent failover**, **operational readiness, and governance.**

Regulators now expect operators to avoid single points of failure, implement automatic failover, and prioritise emergency communications— with auditability and potential penalties for noncompliance.

A practical way forward is to harness satellite as part of a **multi-path, multi-orbit** design—combining terrestrial fibre/5G with satellite—delivering independent failure domains, improved availability, and continuity for mission critical services.

Low Earth orbit (LEO) systems are opening up new and significant opportunities, with **low latency, high throughput** paths that are increasingly offered with enterprise-grade SLAs and APIs.

Existing GEO satellites provide additional coverage and capacity. placing satellite technology at the heart of a new resilience imperative, enhancing service continuity and data assurance.

THE RESILIENCE IMPERATIVE

WHY NOW

Events:
Damage to cable, subsea and overland, have shown how a handful of corridors in the fibre network carry a large share of global data; rerouting raises latency and congestion.

OT/ICS threat escalation:
Nation state and criminal activity targeting utilities, water and energy has grown; ransomware and exploitation of exposed control interfaces continue to rise.

Tightening regulation:
Ofcom's updated guidance and the EU's NIS2 directive formalise resilience duties—risk management, incident reporting, service continuity—with auditability and sanctions.

Service expectations:
Always-on digital interactions make continuity a reputational and economic necessity for public services and enterprises

INTRODUCTION

WHY SATELLITE BELONGS IN A RESILIENCE STRATEGY

For public administration, emergency services, utilities and energy, outages create cascade risk — delays in call handling, impaired situational awareness, and impacts on safety in operational technology environments.

Independent failure domain

Satellite provides path diversity independent of terrestrial last mile and subsea routes; services are rapidly deployable for incident scenes and remote sites.

Complementary orbits

LEO: global, low latency and growing capacity; increasingly offered with enterprise SLAs (e.g., availability credits) and priority tiers.

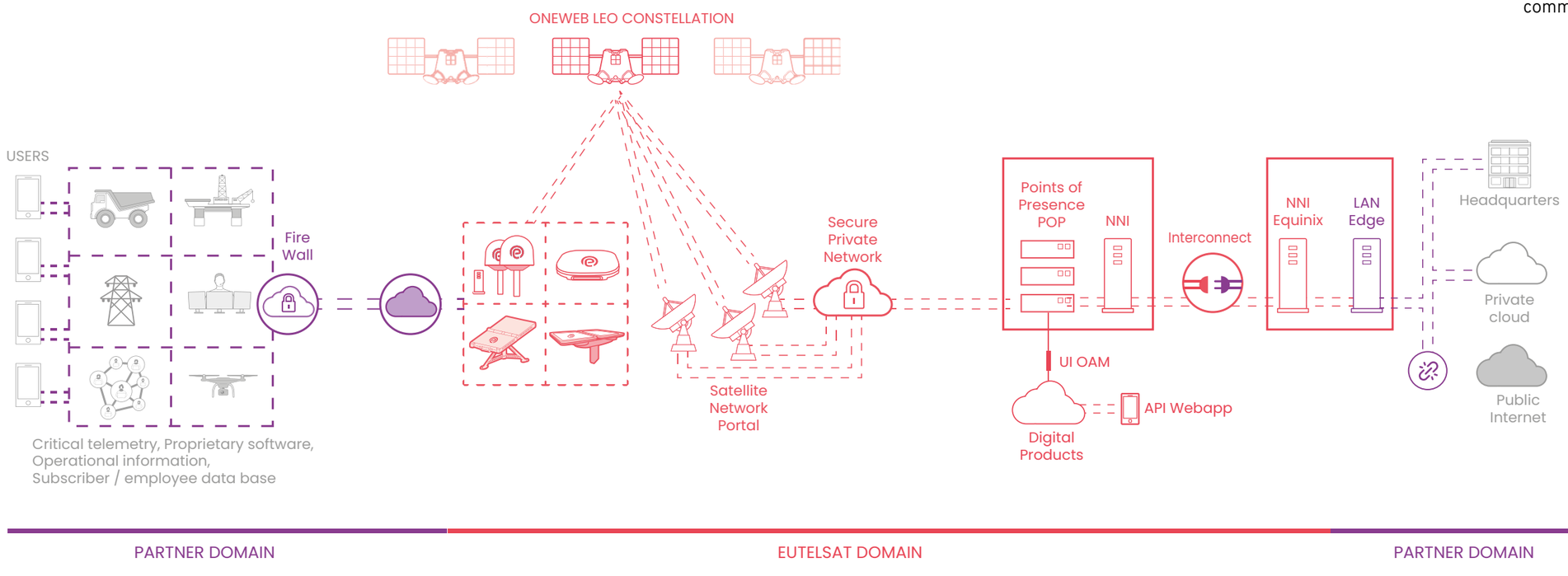
GEO: wide coverage, stable capacity; useful for bulk and scheduled workloads and as a diverse standby.

Standards integration
Regulatory authorities provision for the integration of Non Terrestrial Networks (NTN) into 5G architectures—important for public safety and utilities because it aligns satellite access with cellular identity, QoS and priority frameworks.

WHAT WE MEAN BY NETWORK RESILIENCE (AND WHAT GOOD LOOKS LIKE)

Network resilience is the ability to prevent, withstand, recover from, and adapt to disruptions while maintaining acceptable service levels—measured by availability, latency, jitter, loss and integrity. Resilience spans architecture (diversity, isolation, automation), operations (instrumentation, drills, playbooks) and governance (risk ownership, reporting). Updated official guidance stresses eliminating single points of failure, automatic failover, and priority handling for emergency voice. From redundancy to orchestration.

SYSTEM DIAGRAM ARCHITECTURE



REGULATORY AND STANDARDS LANDSCAPE

UK (Ofcom & Government): Updated network and service resilience guidance: avoid single points of failure, implement automatic failover, test under load, and prioritise emergency services. The UK Resilience Action Plan pushes a whole of society approach across interdependent infrastructures. [ofcom.org.uk], [gov.uk]

EU (NIS2/ENISA): Stronger obligations on essential/important entities, management accountability, and tighter incident reporting; guidance supports technical implementation. [enisa.europa.eu]

Standards (3GPP NTN): Release 17/18 brings satellite into mainstream 5G, enabling supplemental coverage from space and a path to direct to device services over time.

US (Federal Communications Commission): Opens Space Bureau in 2024 to manage the volume of new applications for satellite approvals; recognises satellite's future in national security, critical infrastructure and many aspects of modern life.

LEO ADOPTION, INTEGRATION AND BENEFITS

LEO satellite communications network operators and their Distribution Partners (DPs) have been quick to respond to the new resilient imperative. Connectivity supply is the result of satellite and ground network operations, infrastructure, architecture (diversity, isolation, automation) and governance (risk ownership, reporting) all working together. Commercial services are influenced by varying and competing market forces. Whether the customer solution is backed by Service Level Agreements and CIR for assured network performance will depend on which LEO satellite system the service provider decides to use. The more we embrace LEO technology within the space industry, the more opportunities arise to improve our fibre networks.

LEO HARDWARE AND INSTALLATIONS

The supply, installation and maintenance of satellite antennas is an essential component of any resilient network. Worldclass satellite equipment manufacturers are rapidly developing more ruggedized, more portable and easy-to-install products to enhance and strengthen terrestrial communications networks

Network resilience, where Eutelsat connectivity is a backup in hot-standby or a hybrid link for cellular backhaul, is designed to ensure consistency in communications. In situations where the primary connection fibre may drop then Eutelsat services would take over as directed and transport user traffic back to the DP / carrier. Where there is a legacy VSAT satellite service in place, there is the possibility for latency sensitive or premium data to run over the OneWeb LEO system and regular data over an existing GEO link.

WHY NETWORK RESILIENCE IS GAINING ATTENTION

In a time where digital speed is essential and outages can make headlines, network resilience is emerging as a key pillar of the modern infrastructure strategy.

8.5 million

Number of devices impacted by CrowdStrike glitch in 2024

A routine software update caused what some believe to be the largest tech outage in IT history and highlighted the vulnerabilities in IT infrastructure and the need for robust update management.

The incident caused widespread disruptions across multiple sectors, including critical infrastructure like airports, hospitals, and emergency services, emphasising the interconnected nature of digital supply chains.

Resilience Lessons Learned From the CrowdStrike Incident | SC Media UK

79%

Of telecommunications executives surveyed prioritise their network performance

By not prioritising network modernisation, communications service providers jeopardise the long-term speed and efficiency that can be achieved through enhanced network resilience.

Cloud and AI for a telecom network advantage | IBM

73%

Of businesses acknowledge that fast websites are vital for commercial success

At a minimum, an organisation's digital properties should load as quickly as, or ideally faster than, those of their competitors. Slow-loading websites can lead to frustrated customers, financial losses, and a damaged reputation. To maintain a competitive edge, businesses must ensure reliable resilience that can keep up with the fast-paced changes in the digital landscape.

The Internet Resilience Report 2025

SECTOR TRENDS AND FORECASTS

PUBLIC SERVICES
Today:
National meshes of service centres and access points use terrestrial primary with satellite standby; predictive path switching reduces downtime and supports consistent access to portals and case management platforms.

Forecast:
Expect policy driven orchestration that reallocates capacity during demand peaks (e.g., tax seasons), with LEO terminals standardised for mobile or pop-up service points

EMERGENCY SERVICES
Today:
Deployable command posts operate when cells are down/saturated; satellite integrated vehicle routers support live video, location services and drone telemetry for blue light operations.

Forecast:
Pairing resilient links with AI-assisted situational awareness; progressive adoption of NTN direct-to-device messaging in rugged handsets to maintain communications when both terrestrial and vehicle hubs are impaired.

UTILITIES (POWER, WATER, GRID)
Today:
Remote substations employ managed backup paths for SCADA/telemetry to limit the impact of IT/OT disruptions and aid incident response.

Forecast:
Movement toward dual/tri path (LEO + GEO/MEO + terrestrial) as standard; more edge intelligent substations sharing diagnostics and digital twin updates; self-healing comms fabrics rerouting SCADA traffic under threat or fault signals.

ENERGY EXPLORATION & PRODUCTION

Today:
Offshore/onshore sites require high throughput backhaul for SCADA, video, crew welfare; bulk data steered between GEO and LEO based on latency/cost.

Forecast:
Autonomous multi-orbit traffic engineering will allocate bandwidth by safety criticality and production phase; resilient satellite links will synchronise edge analytics with cloud; unmanned platforms will depend on always on satellite for operations and assurance.

BENEFITS OF MULTI-ORBIT RESILIENCE ARCHITECTURES

Technical

- Independent domains reduce correlated failure: Terrestrial + LEO + GEO lowers exposure to backhaul cuts, power loss, or cable breaks.
- Predictive, session-preserving failover: Real time telemetry (latency, jitter, loss, SiNR) enables hitless switching and materially reduces packet loss versus reactive SD WAN alone.
- Priority protection: Application-aware policies align with guidance to prioritise emergency voice and critical workflows during degradation.
- Standards-based NTN integration: Streamlines identity/QoS mapping and device onboarding into MNO networks.

Operational

- Rapid deployment: Incident scenes and remote assets brought online independent of civil works and damaged terrestrial paths.
- Observability and automation: Telemetry and APIs enable proactive switching ahead of contact gaps; operations get lower MTTR and clearer runbooks.
- Compliance alignment: Documented design, testing and drills support Ofcom/NIS2 compliance.

Strategic

- Continuity as a trust signal: Protects public confidence and revenue by reducing downtime.
- Supply chain resilience: Multi orbit/hybrid mitigates dependency on single vendors or routes.
- Future proofing: Roadmap to NTN direct-to-device and satellite aware SD WAN boosts long term capability growth.

DEPLOYMENT CONSIDERATIONS

By addressing certain fundamental aspects below, businesses and organisations are best able to identify the private network solution most suited to their requirements.

Assumptions

- Spectrum access and site permissions for terminals are achievable; site power resilience (battery/generator) is addressed where required.
- Operations can integrate satellite telemetry into NOC/SD WAN tooling for predictive rather than reactive switching.

Gaps

- Failover remains under tested in many environments; limited telemetry on mean time to restore across hybrid paths. (Industry and academic studies highlight the need for packet order control and hold down logic).
- Policy-driven, predictive switching needed to preserve sessions and QoE under load.
- Not all SD WAN stacks are satellite aware.

RISK

- Simple “backup links” can be insufficient. Satellite behaviours vary for packet ordering and jitter buffering, affecting real time QoE.
- Cost exposure covering terminals, airtime, training and exercises against constrained budgets.
- Vendor lock-in from proprietary terminals or ground segments without standards-based interworking.
- Regulatory hurdles for site permissions, terminal approvals, data routing constraints and export controls.
- Operational complexity in field support (antenna alignment, firmware, cybersecurity), especially at scale.
- Supply-chain and insider threats affecting telecom or utility operations.

KEY RISKS AND MITIGATIONS

With better-informed implementation and strategies around network resilience, customers can reduce risk to a tolerable level, to restrict or eliminate setbacks.

SINGLE DOMAIN FAILURE PERSISTS (TERRESTRIAL ONLY OR SINGLE LEO)

Mitigate:
Engineer tri path diversity (terrestrial + LEO + GEO/MEO) with predictive, session preserving failover and application policies; conduct under load tests.

CYBER COMPROMISE OF EDGE/OT GATEWAYS

Mitigate:
Zero trust segmentation, signed firmware, least privilege access, and out of band satellite management for incident response; align to NIS2 and sector codes.

REGULATORY NON-COMPLIANCE

Mitigate:
Map architecture to Ofcom/NIS2 controls; prioritise emergency voice; maintain power backup at access sites; log drills/incident artefacts.

VENDOR LOCK IN AND OPAQUE SLAs

Mitigate:
Prefer standards aligned NTN; require telemetry APIs, congestion disclosure and SLA remedies; use multi-vendor terminals where practical.

OPERATIONAL COST/SKILLS

Mitigate:
Stage rollouts; central NOC runbooks; training for alignment, power, and cyber hygiene; consider managed multi orbit SD WAN to lower tuning burden.

ACTION LIST FOR DECISIONMAKERS

(NEXT 90–180 DAYS)

- Conduct a resilience feasibility study mapping critical services and single points of failure; quantify outage costs; include subsea route exposure and last mile power risks.
- Pilot multi-orbit at contrasting sites (urban hub for backup; remote site for primary), instrumented for failover time, throughput, latency, jitter and loss; run planned disruption drills.
- Align governance and compliance by gap assessing current practice against Ofcom/NIS2 and sector codes; define evidence artefacts and reporting cadence.
- Update incident playbooks to include satellite activation, roaming/mutual aid coordination, outage transparency and after action reviews.
- Secure supply and skills via dual sourcing terminals, pre-staging spares, and training field teams on installation, power resilience and cyber controls.

WHAT EUTELSAT CAN OFFER

Eutelsat provides a global LEO footprint complemented by GEO capabilities and works through trusted Distribution Partners to design and deliver networks for Aviation, Enterprise, Government, Maritime and Telco markets. Partners can integrate multi orbit connectivity with terrestrial access, leverage Enterprise-grade performance options (e.g., CIR where applicable), and expose telemetry APIs for orchestration and observability—enabling resilient, standards aligned architectures tailored to sector requirements. (For configuration claims such as “hitless failover” and “99.9% availability”, performance depends on site power, antenna placement, and predictive orchestration rather than reactive failover alone.)

NEXT STEPS

CONTACT YOUR EUTELSAT ACCOUNT MANAGER TO EXPLORE REFERENCE DESIGNS, PARTNER ENABLEMENT, AND PILOT OPTIONS.

GLOSSARY

Backhaul:
Connectivity from access nodes such as cell sites to core networks.

Bearer diversity:
Use of multiple independent transmission media to ensure continuity.

DIRS/NORS:
US FCC disaster and outage reporting systems used during emergencies.

Direct-to-Device:
Satellite service that connects standard devices without special terminals.

GEO/LEO/MEO:
Satellite orbits: geostationary, low-Earth and medium-Earth.

GNSS:
Global Navigation Satellite System used for timing and positioning.

Hitless failover:
A switch between paths that does not interrupt active sessions.

IT/OT:
Information Technology and Operational Technology used in industrial control.

Jamming/Spoofing:
Radio interference or fake signal injection targeting satnav or satcom.

Management plane:
Network layer used for configuration and monitoring.

NIS2:
EU directive on network and information systems security.

NTN:
Non-Terrestrial Networks that integrate satellite and HAPS with 5G.

Outage transparency:
Mandated reporting and coordination during failures.

RAN power resilience:
Maintaining radio access service through extended power loss.

Redundancy:
Duplication of components or paths to ensure continuity.

Resilience by design:
Engineering services to tolerate disruption as a core requirement.

SCADA:
Supervisory Control and Data Acquisition used for industrial control.

SD-WAN:
Software defined wide area networking that steers traffic across multiple paths.

TSA (UK):
Telecommunications Security Act and Code of Practice setting security and resilience duties.

CONNECTIVITY_ETL_WP_RESILIENT NETWORK_12P_EN_0326

32 BOULEVARD GALLIENI,
92130 ISSY-LES-MOULINEAUX. FRANCE
WWW.EUTELSAT.COM
+33 1 53 98 47 47

What can we do for you? Please visit
www.eutelsat.com/enquiries